

**Amendments to the Claims**

This listing of claims will replace all prior version, and listings, of claims in the application:

**Listing of Claims:**

1. (Original) A method by which a first computing entity having an RSA key pair  $(N_A, e_A)$ ,  $(N_A, d_A)$  digitally signs and encrypts a message data string,  $m$ , for decryption by a second computing entity having an RSA key pair  $(N_B, e_B)$ ,  $(N_B, d_B)$ , where  $|N_A| = |N_B| = k$  and  $m \in \{0,1\}^n$ , and  $k = n + k_0 + k_1$  for integers  $k_0$  and  $k_1$ , the method comprising:
  - a) selecting an integer  $r \in \{0,1\}^{k_0}$ ,
  - b) computing:
$$w \leftarrow H(C_1(\text{at least } m \text{ and } r))$$
where  $H : \{0,1\}^{n+k_0} \rightarrow \{0,1\}^{k_1}$ , and  $C_1()$  is a deterministic combination function,
  - c) computing:
$$s \leftarrow \text{Enc}(w, C_2(\text{at least } m \text{ and } r))$$
where  $\text{Enc}()$  is a symmetric-key encryption function using  $w$  as key, and  $C_2()$  is a reversible combination function;steps a) to c) being repeated as necessary to obtain  $s || w \leq N_A$ ; and then
  - d) signing by computing:
$$c' \leftarrow (C_3(\text{at least } s \text{ and } w))^{d_A} \bmod N_A$$
where  $C_3()$  is a reversible combination function; and
  - e) if  $c' \leq N_B$ , encrypting  $c'$  by computing:
$$c = c'^{e_B} \bmod N_B.$$
2. (Original) A method according to claim 1, wherein if  $c' > N_B$  following step d), the most significant bit of  $c'$  is removed to obtain a new  $c'$  which is then encrypted by computing:
$$c = c'^{e_B} \bmod N_B.$$

3. (Original) A method according to claim 1, wherein if  $c' > N_B$  following step d), steps a) to d) are repeated as necessary to obtain  $c' \leq N_B$  whereupon  $c'$  is encrypted by computing:

$$c = c'^{c_B} \bmod N_B$$

4. (Original) A method according to claim 1, wherein  $r$  is selected at random.
5. (Original) A method according to claim 1, wherein the function  $C_1()$  is a concatenation function.
6. (Original) A method according to claim 1, wherein the function  $C_2()$  is a concatenation function.
7. (Original) A method according to claim 1, wherein the function  $C_3()$  is a concatenation function.
8. (Original) A method according to claim 1, wherein the functions  $C_1()$ ,  $C_2()$ ,  $C_3()$  are all concatenation functions.
9. (Currently amended) A method according to ~~any one of the preceding claims~~claim 1, wherein the symmetric-key encryption function  $Enc()$  effects at least the ~~followings~~following operations:  
- forming a hash of the key  $w$ ;  
- forming an exclusive-OR of the hash of  $w$  with the output of the combination function  $C_2()$ .
810. (Currently amended) Apparatus for carrying out the method of claim 1.

~~9~~11. (Currently amended) A computer-readable medium storing a computer program arranged to condition a program-controlled computer, when executed by the latter, to carry out the method of claim 1.

~~10~~12. (Currently amended) A method according to claim 1, wherein the second computing entity on receiving  $c$ :

(f) computes:

$$c' \leftarrow c^{d_B} \bmod N_B$$

and, provided  $c' \leq N_A$ , proceeds to the next step;

(g) computes:

$$c'^{e_A} \bmod N_A$$

with the result being subject to a reverse of the combination function  $C_3()$  whereby to recover at least:  $s$  and  $w$ ;

(h) computes:

$$Dec(w, s)$$

where  $Dec()$  is a symmetric-key decryption function complimenting  $Enc()$ , with the result being subject to a reverse of the combination function  $C_2()$  whereby to recover at least:  $m$  and  $r$ ;

(i) checks that the message  $m$  is from the first computing entity by checking that:

$$w = H(C_1(\text{at least } m \text{ and } r)) .$$

~~11~~13. (Currently amended) A system comprising a first computing entity, a second computing entity, and a communications network for communicating the first and second entities, the system being arranged to implement the method of claim ~~10~~12.

~~12~~14. (Currently amended) A method according to claim 2, wherein the second computing entity on receiving  $c$ :

(f) computes:

$$c' \leftarrow c^{d_B} \bmod N_B,$$

and, provided  $c' \leq N_A$ , proceeds to the next step;

(g) computes:

$$c'^{e_A} \bmod N_A$$

with the result being subject to a reverse of the combination function  $C_3()$  whereby to recover at least:  $s$  and  $w$ ;

(h) computes,

$$Dec(w, s)$$

where  $Dec()$  is a symmetric-key decryption function complimenting  $Enc()$ , with the result being subject to a reverse of the combination function  $C_2()$  whereby to recover at least:  $m$  and  $r$ ;

(i) checks that the message  $m$  is from the first computing entity by checking that:

$$w = H(C_1(\text{at least } m \text{ and } r));$$

j) where the check carried out in step (i) fails, computes a new value for  $c'$  as:

$$c' \leftarrow c' + 2^{k-1}$$

and, provided  $c' \leq N_A$ , repeats once steps (g) to (i).

~~13~~15. (Currently amended) A system comprising a first computing entity, a second computing entity, and a communications network for communicating the first and second entities, the system being arranged to implement the method of claim ~~12~~14.

~~14~~16. (Currently amended) A method by which a second computing entity having an RSA key pair  $(N_B, e_B)$ ,  $(N_B, d_B)$ , decrypts and authenticates a ciphertext  $c$  that is purportedly a signed and encrypted form produced by a first computing entity of a message data string  $m$ , the first computing entity having an RSA key pair  $(N_A, e_A)$ ,  $(N_A, d_A)$  where  $|N_A| = |N_B| = k$  and  $m \in \{0,1\}^n$ , and  $k = n + k_0 + k_1$  for integers  $k_0$  and  $k_1$ ; the second computing entity on receiving  $c$ :

(a) computes:

$$c' \leftarrow c^{d_B} \bmod N_B$$

and proceeds to the next step provided that  $c' \leq N_A$ ;

(b) computes:

$$c'^{e_A} \bmod N_A$$

with at least quantities  $s$  and  $w$  being recovered from the result;

(c) computes:

$$Dec(w, s)$$

where  $Dec()$  is a symmetric-key decryption function complementing  $Enc()$ , with at least quantities  $m$  and  $r$  being recovered from the result;

(d) checks that the message  $m$  is from the first computing entity by checking that:

$$w = H(C_I(\text{at least } m \text{ and } r))$$

where  $H : \{0,1\}^{n+k_0} \rightarrow \{0,1\}^{k_1}$  and  $C_I()$  is a deterministic combination function.

~~15~~17. (Currently amended) A method according to claim ~~14~~16, wherein the function  $C_I()$  is a concatenation function.

~~16~~18. (Currently amended) A method according to claim ~~14~~16, wherein the symmetric-key decryption function  $Dec()$  effects at least the followings operations:

- forming a hash of the key  $w$ ;
- forming an exclusive-OR of the hash of  $w$  with  $s$ .

~~17~~19. (Currently amended) Apparatus for carrying out the method of claim ~~14~~16.

~~18~~20. (Currently amended) A computer-readable medium storing a computer program arranged to condition a program-controlled. computer, when executed by the latter, to carry out the method of claim ~~14~~16.

~~19~~21. (Currently amended) A method by which a first computing entity having an RSA key pair  $(N_A, e_A)$ ,  $(N_A, d_A)$  digitally signs and encrypts a message data string,  $m$ , for decryption by a second computing entity having an RSA key pair  $(N_B, e_B)$ ,  $(N_B, d_B)$ , where  $|N_A| = |N_B| = k$  and  $m \in \{0,1\}^n$ , and  $k = n + k_0 + k_I$  for integers  $k_0$  and  $k_I$ , the method comprising:

- a) selecting an integer  $r \in \{0,1\}^{k_0}$ ,
  - b) forming the hash  $\omega = H(m \parallel r)$  where  $H: \{0,1\}^{n+k_0} \rightarrow \{0,1\}^{k_1}$ , and
  - c) forming the hash  $s = G(\omega) \oplus (m \parallel r)$  where  $G: \{0,1\}^{k_1} \rightarrow \{0,1\}^{n+k_0}$ ;
- steps a) to c) being repeated as necessary to obtain  $s \parallel \omega \leq N_A$ ; and then
- d) signing by forming  $c' = (s \parallel \omega)^{d_A} \bmod N_A$ ; and, if  $c' > N_B$ , removing the most significant bit of  $c'$  to obtain a new  $c'$ ; and then
  - e) encrypting  $c'$  by forming  $c = c'^{e_B} \bmod N_B$ .

~~20~~22. (Currently amended) The method as claimed in claim ~~19~~21 in which  $r$  is selected at random.

~~21~~23. (Currently amended) A computer storage medium having stored thereon a computer program readable by a general-purpose computer, the computer program including instructions for said general purpose computer to configure it for implementing the steps of the method of claim ~~19~~21.

~~22~~24. (Currently amended) A method by which a first computing entity having an RSA key pair  $(N_A, e_A)$ ,  $(N_A, d_A)$  digitally signs and encrypts a message data string,  $m$ , for decryption by a second computing entity having an RSA key pair  $(N_B, e_B)$ ,  $(N_B, d_B)$  where  $|N_A| = |N_B| = k$  and  $m \in \{0,1\}^n$ , and  $k = n + k_0 + k_1$  for integers  $k_0$  and  $k_1$ ; the method comprising:

- a) selecting an integer  $r \in \{0,1\}^{k_0}$ ,
  - b) forming the hash  $\omega = H(m \parallel r)$  where  $H: \{0,1\}^{n+k_0} \rightarrow \{0,1\}^{k_1}$ , and
  - c) forming the hash  $s = G(\omega) \oplus (m \parallel r)$  where  $G: \{0,1\}^{k_1} \rightarrow \{0,1\}^{n+k_0}$ ;
- steps a) to c) being repeated as necessary to obtain  $s \parallel \omega \leq N_A$  and then
- d) signing by forming  $c' = (s \parallel \omega)^{d_A} \bmod N_A$ ;
- steps a0 to d) being repeated as necessary to obtain  $c' < N_B$ , and then
- e) encrypting  $c'$  by forming  $c = c'^{e_B} \bmod N_B$ .

- ~~23~~25. (Currently amended) The method as claimed in claim ~~22-24~~ in which  $r$  is selected at random.
- ~~24~~26. (Currently amended) A computer storage medium having stored thereon a computer program readable by a general-purpose computer, the computer program including instructions for said general purpose computer to configure it for implementing the steps of the method of claim ~~22~~24.